

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION**

CENTRIPETAL NETWORKS, LLC,

Plaintiff,

V.

CISCO SYSTEMS, INC.,

Defendant.

No. 2:18-cv-00094-EWH-LRL

PUBLIC VERSION - REDACTED

PLAINTIFF CENTRIPETAL NETWORKS, LLC'S TRIAL BRIEF

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. BACKGROUND	1
A. Centripetal Patented Its Inventions for Operationalizing Threat Intelligence.....	1
B. Cisco Came to Centripetal for Its Patented Solution	2
C. Cisco Incorporated Centripetal’s Patented Technologies into Its Products	3
D. Centripetal Presented Ample Evidence of Cisco’s Willful Infringement and Its Resulting Damages at Trial	6
III. CISCO WILLFULLY INFRINGES CENTRIPETAL’S ASSERTED PATENTS.....	9
A. Cisco Infringes Claims 18 and 19 of the ’193 Patent	9
B. Cisco Infringes Claims 9 and 17 of the ’806 Patent	11
C. Cisco Infringes Claims 11 and 21 of the ’176 Patent	13
D. Cisco Infringes Claims 24 and 25 of the ’856 Patent	14
IV. CENTRIPETAL’S ASSERTED PATENTS ARE VALID AND ENFORCEABLE.....	17
A. Cisco Took the Position at Trial that All of the Accused Products Used Old Technology	18
B. The Asserted Claims Are Valid Because Cisco Failed to Address Claim Elements.....	19
1. The ’193 Patent is Valid	20
2. The ’806 Patent is Valid	20
3. The ’176 Patent is Valid	21
4. The ’856 Patent is Valid	21
C. Cisco’s Experts Are Not Credible Because They Applied Differing Claim Constructions	22
D. Cisco Defense of Written Description Fails	23

1.	Written Description Defense Requires a POSITA.....	23
2.	The '856 and '176 Patents Convey with “Reasonable Certainty” All Claims Elements	24
V.	CENTRIPETAL IS ENTITLED TO RELIEF FOR CISCO’S WILLFUL INFRINGEMENT.....	25
A.	Centripetal Demonstrated a Reasonable Royalty Apportioned to the Footprint of the Invention	25
B.	Cisco’s Willful Infringement Warrants Additional Relief, including Enhanced Damages and a Permanent Injunction.....	29
VI.	CONCLUSION.....	30

TABLE OF AUTHORITIES**Page(s)****Cases**

<i>Alcon Rsch. Ltd. v. Barr Labs., Inc.</i> , 745 F.3d 1180 (Fed. Cir. 2014).....	23
<i>Biogen Int’l GmbH v. Mylan Pharms. Inc.</i> , 18 F.4th 1333 (Fed. Cir. 2021)	24
<i>Elbit Sys. Land & C4I Ltd. v. Hughes Network Sys., LLC</i> , 927 F.3d 1292 (Fed. Cir. 2019).....	28
<i>Finjan, Inc. v. Blue Coat Sys., Inc.</i> , 879 F.3d 1299 (Fed. Cir. 2018).....	27
<i>Georgetown Rail Equip. Co. v. Holland L.P.</i> , 867 F.3d 1229 (Fed. Cir. 2017).....	29
<i>Halo Elecs., Inc. v. Pulse Elecs., Inc.</i> , 579 U.S. 93 (2016).....	29
<i>Idenix Pharms. LLC v. Gilead Scis. Inc.</i> , 941 F.3d 1149 (Fed. Cir. 2019).....	24
<i>Immersion Corp. v. Sony Comput. Ent. Am., Inc.</i> , No. C 02-0710 CW, 2005 U.S. Dist. LEXIS 4777 (N.D. Cal. Jan. 10, 2005).....	27
<i>Kimberly-Clark Corp. v. Johnson & Johnson</i> , 745 F.2d 1437 (Fed. Cir. 1984).....	22
<i>Microsoft Corp. v. i4i Ltd. P’ship</i> , 564 U.S. 91 (2011).....	17
<i>Miller v. Genie Indus., Inc.</i> , No. 3:10-cv-00063-MPM-SAA, 2012 WL 161408 (N.D. Miss. Jan. 19, 2012)	23
<i>Read Corp. v. Portec, Inc.</i> , 970 F.2d 816 (Fed. Cir. 1992).....	29
<i>Serby v. First Alert, Inc.</i> , 134 F. Supp. 3d 668 (E.D.N.Y. 2015), <i>vacated on other grounds</i> , 664 F. App’x 105 (2d Cir. 2016), <i>as amended</i> (Dec. 22, 2016)	23, 24
<i>Streck, Inc. v. Rsch. & Diagnostic Sys., Inc.</i> , 665 F.3d 1269 (Fed. Cir. 2012).....	24

Vectura Ltd. v. GlaxoSmithKline LLC,
981 F.3d 1030 (Fed. Cir. 2020).....28

W.L. Gore & Assocs., Inc. v. Garlock, Inc.,
842 F.2d 1275 (Fed. Cir. 1988).....22

WesternGeco L.L.C. v. ION Geophysical Corp.,
837 F.3d 1358 (Fed. Cir. 2016).....29

Statutes

35 U.S.C. § 282.....17

35 U.S.C. § 284.....25, 29

I. INTRODUCTION

Over the course of a 23-day trial, Centripetal proved that Cisco copied its groundbreaking patented technology that differentiated it from all existing security solutions. After signing a non-disclosure agreement with Centripetal, Cisco met with Centripetal under the guise of partnering with the much smaller company. During these meetings, Cisco sought technological details and the “algorithms” that made Centripetal’s patented products a novel and unique solution to a complex problem. Cisco’s next move was to steal Centripetal’s patented technology, implementing this technology in its networking equipment that had become commodity products and announcing to the world that with this new technology, Cisco’s infringing products were the “network of the future.” *See, e.g.*, Tr. at 892:23-893:18 (citing PTX-452 at 648).

Cisco announced that its new networking products, focused on Centripetal’s patented cybersecurity solutions, “represent one of the most significant breakthroughs in enterprise networking” and “solve[] a network security challenge previously thought to be unsolvable.” PTX-452 at 648. As a result of Cisco’s willful infringement of Centripetal’s patents, Cisco reaped great financial benefits. When Cisco unveiled its networking products that focused on security, its revenues for its infringing products hit record numbers (*e.g.*, “Cisco More Than Doubles its Catalyst 9000 Customer Base” and was the “fastest ramping product in Cisco’s history.”). Tr. at 3113:15-3114:13 (citing PTX-515 at 426). And because of this new focus on security, Cisco has maintained astronomical revenues for its infringing products.

As reflected in the trial record, Cisco’s own documents and engineers’ testimony provided uncontroverted evidence of Cisco’s willful infringement of Centripetal’s patents.

II. BACKGROUND

A. Centripetal Patented Its Inventions for Operationalizing Threat Intelligence

In 2009, decorated veterans Steven Rogers and his son Jonathan Rogers founded

Centripetal to develop a new solution to leverage Cyber Threat Intelligence (“CTI”) to detect and stop cybersecurity threats. After investing \$65 million in research and development, Centripetal launched RuleGATE which used CTI to improve network security drastically. Tr. at 1202:23-1203:5. Centripetal recognized the novelty of its technology and filed for patents, marking its RuleGATE with its patents. Tr. at 1203:12-1204:3, PTX-528; Tr. 1383:18-1385:19, PTX-1215.

B. Cisco Came to Centripetal for Its Patented Solution

Facing commoditization of its bread-and-butter network devices, Cisco needed a differentiator. Tr. at 1452:3-21 (2016 10-K describing “increased competition . . . based on commoditized hardware”). In 2015, it saw Centripetal’s patented technology as a solution that “fit into the types of solutions [Cisco] needed for customers . . . that went beyond the offerings that Cisco had at the time” and contacted Steven Rogers to learn more about this technology. Tr. at 256:8-257:12. Centripetal and Cisco signed an NDA to explore jointly selling Centripetal’s technology in Cisco products. Tr. at 1213:16-20, 1214:3-20; PTX-99. Centripetal and Cisco had several meetings, including those with Cisco’s technical and corporate development teams, where Centripetal provided multiple confidential demonstrations of RuleGATE and its patented technology. PTX-547 at 389-91; Tr. at 258:21-25, 260:2-18, 1219:22-1222:25, 1223:23-1224:22, 1225:11-1227:18 (citing PTX-102). At Cisco’s invitation, Centripetal also presented its patented solution at the Cisco Live conference as Cisco’s technology partner. Tr. at 1298:1-24; *see also* Tr. at 1024:16-25. Over an eighteen-month period when Cisco purported to be interested in a partnership, Cisco’s employees were combing through Centripetal’s website for additional information, accessing over 1,200 web pages over the course of 354 visits. Tr. at 1024:16-25.

Centripetal also disclosed substantial confidential information to Cisco during their meetings. At a February 2016 meeting, Centripetal presented detailed, highly sensitive, confidential and proprietary information about its patented technology and products, including its

patented filter algorithms to prevent exfiltration ('193 Patent), correlation algorithms ('176 Patent) and Centripetal's patented technologies for detecting threats in encrypted traffic ('856 Patent), and rule swapping ('806 Patent). Tr. at 1219:15-1224:22; PTX-547 at 389-91.

Centripetal answered various questions about its patented technologies at the meeting. Tr. at 1225:12-16, 1227:9-18. Contemporaneous documents confirmed these disclosures, including emails to Cisco from Jonathan Rogers, Centripetal's VP of Operations at the time, noting that the Cisco team "hone[d] in on our filter technology & algorithms" and asked "questions on our patents." Tr. at 1226:10-1227:18; PTX-102 at 1. After that meeting, a Cisco engineer told his team to "look at [Centripetal's] algorithms" and "study their [patent] claims." Tr. at 1128:8-1129:5; PTX-134 at 3. Cisco received additional Centripetal confidential information through late 2016, including a list of Centripetal's issued patents, patent-practicing products, and highly sensitive technical disclosures detailing RuleGATE's core patented functionalities. Tr. at 1235:11-1236:21, 1237:25-1238:19; 1242:11-1243:10; DTX-1270 at 1, 25, 27-28, 30.

C. Cisco Incorporated Centripetal's Patented Technologies into Its Products

After learning about Centripetal's threat-intelligence-based security, Cisco, in June 2017, unveiled its "network of the future" that "stops security threats in their tracks." Tr. at 1159:9-1161:5 (citing PTX-452 at 648). Cisco launched its new router, switch, and firewall, which integrated "built-in" security to make and enforce rules protecting against network threats, nearly two years after its first meeting and within six months after its last meeting with Centripetal. *See, e.g.*, Tr. at 733:3-734:22 (citing PTX-585 at 410).

A description of Cisco's infringing technology is provided below:

Catalyst 9000 Switch: Cisco introduced a “new family of switches built from the ground up” termed the “Catalyst 9000 Switch”¹ that was designed to “deliver[] unmatched security.” Tr. at 1160:8-1161:5 (citing PTX-452 at 649). The Catalyst 9000 Switch, launched in June 2017, was “built for security” and “designed to enable customers to detect threats, for instance, in encrypted traffic” as part of “a critical part of an end-to-end integrated security solution, one that detects and stops threats.” PTX-1260 at 849; PTX-1449 at 884.

ISR/ASR Router: Cisco introduced the same security features in its new Catalyst 9000 Switch into its Integrated Services Router (“ISR”) and Aggregation Services Router (“ASR”) family of routers (“ISR/ASR Router”²) by updating its software on July 3, 2017, to enforce network security rules that forward or drop packets. Tr. at 443:17-444:10; PTX-1195 at 1. Cisco explained that its ISR/ASR Router now “include[s] integrated security, advanced analytics, automated provisioning, and application optimization, to deliver a complete solution.” PTX-1226 at 638 (discussed in Tr. at 443:17-444:10).

DNA Center: Cisco integrated its Digital Network Architecture (“DNA”) technology into its Catalyst 9000 Switch and ISR/ASR Router, allowing its DNA Center to manage them with rules. Tr. at 576:25-577:8, 579:10-580:24; PTX-1263 at 179; PTX-1294 at 3. DNA Center pre-processes rule sets, which Catalyst Switch and ISR/ASR Router can swap in without packet loss. Tr. at 597:13-602:2; PTX-1195 at 3-4. DNA Center’s primary function is to interact and operate routers and switches providing the infringing capabilities. Tr. at 55:13-21, 147:19-21.

¹ Cisco’s Catalyst 9000 Switch includes the Catalyst 9300, 9400, 9500, and 9800 series running IOS-XE 16.5 and subsequent releases and the controller running IOS-XE 16.10 and subsequent releases. Tr. at 434:14-17.

² Cisco’s ISR/ASR Router includes the 1000 and 4000 series ISR and 1000 series ASR router running IOS-XE 16.5 and subsequent versions infringe. Tr. at 433:24- 434:1.

Stealthwatch: Cisco upgraded its Stealthwatch software that included, *inter alia*, a technology termed Cognitive Threat Analytics (“CTA”) in 2017 to analyze traffic flowing through the Catalyst 9000 Switch and ISR/ASR Router to “detect and respond to threats in real-time.” Tr. at 2342:4-7; PTX-482 at 664; PTX-577 at 007; PTX-992 at 1-2; *see, e.g.*, Tr. at 2148:8-25 (explaining the differences in release numbers for Stealthwatch, noting that CTA was added to Stealthwatch in 2017). This analysis involves correlating traffic that enters and leaves devices in the network to determine whether the traffic contains a threat. Tr. at 994:18-995:21; PTX-1065 at 5. Detected malicious traffic can be “blocked or quarantined by Stealthwatch,” which involves sending rules to Catalyst 9000 Switch and ISR/ASR Router. PTX-584 at 403. Cisco touts Stealthwatch as a “feature” of its Catalyst 9000 Switch and ISR/ASR Router and sells them “as one product.” Tr. at 1463:22-1464:16; PTX-1507 at 495.

ETA: In late 2017, Cisco introduced Encrypted Traffic Analytics (“ETA”) into its new Catalyst 9000 Switch and ISR/ASR Router to protect against threats in encrypted traffic without needing to decrypt the traffic. Tr. at 61:17-24; Tr. at 887:18-888:11; 890:10-22 (testimony regarding PTX-561 at 630); PTX-20 at 2 (functionality “built in to the system”); deposition testimony of Saravanan Radhakrishnan (PTX-1906) at 55:25-56:9. Cisco touts ETA as a “feature” of and “[b]enefit of [u]pgrading to” its redesigned Catalyst 9000 Switch and ISR/ASR Router. PTX-1260 at 849; PTX-1248 at 265-66; PTX-1507 at 495.

ISE: Cisco’s Identity Services Engine (“ISE”) software provides “[c]entral network device management” and “granular control of who can access which network device.” PTX-411 at 891. Stealthwatch and ISE “work together” as “an integrated solution.” Tr. at 1466:18-1467:11 (citing PTX-1035 at 1-2); *see also* PTX-563 at 415. ISE can generate rules enforced by Catalyst 9000 Switch and ISR/ASR Router to protect networks from threats, even in encrypted traffic.

Firewall: Cisco designed a new architecture for its Adaptive Security Appliance (“ASA”) Firewalls with Firepower and its Firepower Appliance Firewalls³ around late 2017 by adding Threat Intelligence Director (“TID”) to the Firepower Management Center (“FMC”). Tr. at 558:1-20. Cisco’s Firewalls provide a new level of network security based on threat indicators with new rules that can be swapped efficiently in the devices. Tr. at 694:13-695:9.

FMC: Cisco designed a new management software for its Firewalls integrating them with FMC version 6.0 and later. The FMC also includes TID, which receives rules from various sources and preprocesses them into a rule set. Tr. at 558:1-20.

Cisco’s “Network of the Future” enjoyed great success by relying on Centripetal’s patented technologies. A table of Centripetal’s Patents along with Cisco’s infringing products (collectively, “Accused Products”) is below:

Centripetal’s Patent	Accused Cisco Products
’193 Patent	Catalyst 9000 Switch
	ISR/ASR Router
’806 Patent	Catalyst 9000 Switch with DNA Center
	ISR/ASR Router with DNA Center
	Firepower/Adaptive Security Appliance Firewall with Firepower Management Center
’176 Patent	Catalyst 9000 Switch with Stealthwatch
	ISR/ASR Router with Stealthwatch
’856 Patent	Catalyst 9000 Switch with Stealthwatch and ISE
	ISR/ASR Router with Stealthwatch and ISE

D. Centripetal Presented Ample Evidence of Cisco’s Willful Infringement and Its Resulting Damages at Trial

During the 23-day bench trial that included 35 witnesses, over 300 exhibits, and 3,500 transcript pages, Centripetal presented overwhelming evidence of Cisco’s willful infringement,

³ The accused ASA firewalls include Cisco’s Adaptive Security Appliance 5500 with Firepower services (version 9.4 and later). The accused Firepower firewalls include Cisco’s Firepower Appliance 1000, 2100, 4100, and 9300 series that run Firepower Threat Defense 6.0 and later. Centripetal collectively refers to these accused products as “Firewalls.”

the appropriate remedies, and soundly rebutted Cisco's invalidity allegations. Centripetal presented several technical experts in cybersecurity and computer networking. Dr. Medvidovic provided a tutorial and opined on the importance of the patented technology to the Accused Products. Dr. Mitzenmacher opined on the infringement of the '193 and '806 Patents. Dr. Cole opined on the infringement of the '176 and '856 Patents. Dr. Striegel opined on apportionment between infringing and non-infringing functions of the Accused Products. Centripetal's damages expert, Mr. Gunderson, testified regarding a reasonable royalty for past damages. Finally, Mr. Malackowski, an expert in intellectual property valuation and patent licensing, testified regarding the impact of Cisco's infringement on Centripetal today and in the future, supporting a permanent injunction. Finally, to rebut Cisco's invalidity allegations, Dr. Orso opined on the validity of the '193 and '806 Patents, Dr. Jaeger opined on the validity of the '176 and '856 Patents, and Dr. Striegel returned to opine on secondary considerations of non-obviousness.

Cisco and its experts took multiple credibility-shredding "heads-I-win, tails-you-lose" positions at trial that were inconsistent. Cisco's technical experts – a different expert for each patent – testified that the accused technology did not infringe the asserted patent, while simultaneously taking the position that if it did infringe the patent, then the patent is invalid because all of Cisco's technology is old technology that has been around for years. To maintain such positions, Cisco's experts were forced to contradict Cisco's engineers and documents. *See, e.g.,* Tr. at 1898:19-21 (The Court observed, "[I]t's clear to the Court that either what the ads say is wrong or what the witness [Cisco expert Dr. Schmidt] says is wrong. They can't both be right."). For example, Cisco's expert, Dr. Reddy, created an animation that conflicted with Cisco's technical documents and engineers, opining that rules were only applied by the products for packets entering ("ingress") the product and not when exiting ("egress") the product. Tr. at

2615:2-2619:13. In actuality, all evidence showed that rules were applied both at the ingress and egress. Tr. at 2568:5-16, 2568:21-24 (fact witness); DTX-562 at 43.

Cisco's validity position required it to argue that its products had the same technology for years, despite Cisco's repeated claims—including those made under penalty of law—about its much-touted revolutionary network security, claiming at trial that the highly-successful Accused Products were identical to its old equipment. *Compare, e.g.*, Tr. at 2100:12-2101:18 (Cisco's expert testifying that he assumed the Catalyst 9000 Switch met the asserted claims of the '856 Patent and wrongly asserting that the '856 Patent "covers" use of decryption hardware) *with* PTX-1417 at 107 (Catalyst 9000 Switch guide explaining that "[b]efore the introduction of the Catalyst 9000 series," detecting attacks in encrypted traffic "meant installing decryption hardware" which the new Catalyst 9000 Switch do not need); *compare* PTX-1135 at 946 (heralding Cisco's Encrypted Traffic Analytics functionality that "solves" a "challenge previously thought to be unsolvable") *with* Tr. at 2105:1-2106:4 (Cisco's expert claiming ETA was a minor fringe improvement, and it was "possible for [Cisco] to do [encrypted traffic analysis] before that").

Cisco's damages position was equally untenable because it claimed that it did not sell the Accused Products as integrated systems, despite Cisco's public representations and the testimony of its own expert that infringing functionality was "embedded" in the product, and that "[o]nly . . . those customers [that] are extremely looking forward to having their networks hacked" would fail to use Cisco's "[c]omprehensive set of products." Tr. at 2130:7-20, 2131:12-22; *see also* PTX-963 at 783. Cisco also claimed that the total value of the '193, '806, '176, and '856 Patents was \$3,014,561 because the accused functionality was of minimal value—a figure less than the

\$3.86 million that Cisco stated was the cost of a *single* data breach. PTX-584 at 398; DTX-1693 at 1.

III. CISCO WILLFULLY INFRINGES CENTRIPETAL'S ASSERTED PATENTS

A. Cisco Infringes Claims 18 and 19 of the '193 Patent

The '193 Patent, referred to as the “Forward or Drop/Exfiltration Patent” at trial, relates to using rules to filter packets depending on the type of data transfer. Tr. at 468:18-469:9, 2356:2-6. The '193 Patent protects against cybercriminals using dangerous security breaches called exfiltration attacks to hijack computers on a network and steal (“exfiltrate”) data. Tr. at 343:12-16, 465:16-21. To do this, the '193 Patent prevents potentially compromised computers from making a particular type of data transfer (*e.g.*, accessing a company’s sensitive data) while allowing other types of data transfers (*e.g.*, accessing the Internet). Tr. at 467:14-469:9. This stops the data from being exfiltrated to the cyber criminals, leaving them with nothing.

In proving that Cisco’s Catalyst 9000 Switch and separately, its ISR/ASR Router infringe the '193 Patent, Centripetal’s expert, Dr. Mitzenmacher, relied on twenty-two (22) trial exhibits that included Cisco’s confidential documents and source code. He also relied on the sworn testimony of Cisco’s engineers which confirmed the functionality of Cisco’s Catalyst 9000 Switch and ISR/ASR Router. *See e.g.*, deposition testimony of Peter Cernohorsky (PTX-1911) at 48:21-49:16; Peter Jones (PTX-1912, PTX-1913) at 27:12-28:2, 30:23-31:20; and Martin Hughes (PTX-1914) at 40:9-19. Tellingly, Cisco’s confidential documents, and engineers contradict Cisco’s expert at trial on the functionality of Cisco’s Catalyst 9000 Switch and ISR/ASR Router. It is likely because of this overwhelming infringement evidence that Cisco only contested infringement of one claim element at trial—the third element starting with the “responsive to a determination” language. Within that claim element, Cisco contested whether its Catalyst 9000 Switch and ISR/ASR Router had “one or more packet-filtering rules configured to

prevent a particular type of data transfer from the first network to a second network” as recited in the ’193 Patent’s Asserted Claims. Thus, infringement hinged on whether Cisco’s Catalyst 9000 Switch and ISR/ASR Router had packet-filtering rules.

The technology in Cisco’s Catalyst 9000 Switch and ISR/ASR Router that was proved to infringe the ’193 Patent was its enhanced “Quarantine” security feature. Tr. at 433:16-434:1. As the name implies, the Quarantine technology prevents certain computers from accessing sensitive information. The Quarantine technology applies rules and Secure Group Tag/Scalable Group Tag (“SGTs”) to packets based on information including protocol and ports used. Tr. at 494:12-24; PTX-1276 at 211. The Quarantine technology in the Catalyst 9000 Switch and ISR/ASR Router then uses access control rules, e.g., the Group Access Control List (“GACL”), specific security rules called Security Group ACL (“SGACL”) based on the SGTs, to control access to specific resources. PTX-1390 at 86.

The Quarantine feature works when the ACL rules, including the SGACL rules, show that a packet is tagged and should be blocked. PTX-1276 at 216; Tr. at 2419:16-2422:1. A Quarantine rule directs the blocking of packets to isolate an infected computer from sensitive information. Tr. at 527:4-22; PTX-1326 at 011. The Quarantine rule prevents particular types of data transfers to or from potentially compromised computers—*e.g.*, transfers involving networks with sensitive information—but allow transfers involving other networks, such as the Internet. Tr. at 541:12-542:16 (testimony regarding Cisco presentation (PTX-563 at 415) illustrating in color blocking access (red) or allowing access (green) to certain types of data); Tr. at 547:1-548:19 (the Catalyst 9000 Switch and ISR/ASR Router apply rules to drop or forward packets associated with a particular “type of data transfer”). As Cisco’s documents state, “[d]evices that are suspected of being infected can be denied access to critical data while their users can keep

working on less critical applications.” PTX-1326 at 11. Other traffic to or from the compromised computer’s network is not affected.

In order to gin up non-infringement defenses, Cisco resorted to:

- (1) rewriting the claims to add new and different criteria to the claim language of the contested element by adding an inspection step instead of the prevention step
- (2) adding additional products to Centripetal’s infringement allegations – *i.e.*, not just the Catalyst 9000 Switch or ISR/ASR Router by themselves as Centripetal alleged, but also adding the ISE and Stealthwatch products in combination with the Catalyst 9000 Switch or ISR/ASR Router as accused products.

As demonstrated by the trial record and outlined in Centripetal’s Renewed Findings of Fact and Conclusions of Law, this manufactured non-infringement position is without factual or legal support.

B. Cisco Infringes Claims 9 and 17 of the ’806 Patent

The ’806 Patent, referred to as the “Rule Swap Patent” at trial, improves how network devices use rules to monitor and filter (*e.g.*, block or drop) network traffic. Tr. at 338:19-340:1. Because cyber threats evolve rapidly, these rules require frequent updates. Tr. at 339:5-340:1. Centripetal recognized that “[a]s rule sets increase in complexity, the time required for switching between them presents obstacles for effective implementation,” often resulting in dropped packets. ’806 Patent at 1:20-22. To address this, the ’806 Patent preprocesses the rules so it can perform rule swaps in between the processing of packets to ensure none are dropped. *Id.* at 4:60-64, 11:40-53.

Dr. Mitzenmacher relied on twenty-six (26) trial exhibits and the sworn testimony of Cisco’s engineers to demonstrate that Cisco’s Catalyst 9000 Switch and ISR/ASR Router in combination with DNA Center infringe the ’806 Patent. Tr. at 641:3-24. DNA Center receives threat intelligence feeds, operationalizes them, and turns them into new rules and policies for the Catalyst 9000 Switch and ISR/ASR Router. Tr. at 450:23-451:24; PTX-1294 at 3. The Catalyst

9000 Switch and ISR/ASR Router receive and implement these new rules (rule swapping) from the DNA Center without dropping any packets using a technology known as Hitless ACL for FED 2.0. Tr. at 575:15-577:8, 579:18-580:24, 584:14-585:4, 586:15-587:18, 588:12-589:18; PTX-1294 at 3; PTX-1195 at 3-4 (describing Hitless ACL for FED 2.0). This technology directs the processor in the products (the “UADP processor”) to cease their processing of packets, swap the rule set using a cache, and resume processing based on a signal. Tr. at 597:10-601:8, 606:15-608:14, 633:24-634:14; DTX-562 at 43 (showing UADP processor in the Catalyst 9000 Switch and ISR/ASR Router that is used to swap rules). The Cisco engineer that designed this technology provided the following infringement-affirming testimony during cross-examination:

'806 Patent – Claim 9	Peter Jones' Trial Testimony (Tr. at 2571:12-2573:8)
receive a first rule set and a second rule set;	Q. Now, the Catalyst switches, they can receive rule sets from a variety of sources; isn't that right? A. That is correct. Q. And one of those sources can be the DNA center; isn't that right? A. Yes, they may receive rules from the DNA center.
preprocess the first rule set and the second rule set to optimize performance of the system for processing packets in accordance with at least one of the first rule set or the second rule set;	Q. And, now, the way the Catalyst processes these rules, in order to process these rules, the Catalyst switch must compile them, right, in order to implement the rules? A. That is correct.
configure at least two processors of the plurality of processors to process packets in accordance with the first rule set;	Q. And in doing this compiling, it compiles these rules while the old rule set is still processing packets, while the old rules are still being applied to packets; isn't that right? A. That is correct.
after preprocessing the first rule set and the second rule set and configuring the at least two processors to process packets in accordance with the first rule set, receive a plurality of packets;	
process, in accordance with the first rule set, a portion of the plurality of packets;	
signal, each processor of the at least two processors, to process packets in accordance with the second rule set; and	Q. Now, once the compilation is complete, a signal is sent to the processor to stop processing packets with the old rule set and to start processing packets with the new rule set; isn't that right? A. That is correct.
configure, each processor of the at least two processors to, responsive to being signaled to process packets in accordance with the second rule set:	
cease processing of one or more packets;	Q. And then during the two to four clock periods that you mentioned yesterday, when there's no processing of packets, the rules are swapped; isn't that right? A. That is correct. There is -- the processing of packets continues. Packets are processed at a maximum frequency of two to four clock periods. So we don't stop processing the packets, there's just an idle period between two packets.
cache the one or more packets;	Q. But there's a signal that's sent to say, stop processing packets with the old rule set and start processing packets with the new rule set, correct? A. Yes, we swap from the old to the new.
reconfigure to process packets in accordance with the second rule set;	Q. And you do that swap in between -- in that two to four clock cycles that you mentioned yesterday, correct? A. Right.
signal completion of reconfiguration to process packets in accordance with the second rule set; and	Q. Now, once that process is complete, the system signals that the swap has been complete, and then the new rule set will be applied to any subsequent packet; isn't that right? A. We don't -- we don't signal that a swap is complete, we just instruct the swap to happen.
responsive to receiving signaling that each other processor of the at least two processors has completed reconfiguration to process packets in accordance with the second rule set, process, in accordance with the second rule set, the one or more packets.	Q. Well, there's a return success that happens after the swap is complete, correct? A. There's really not. We just do a write of the new value. So it's a memory write. Q. A memory write, okay. But in the document, it actually says that you return success. That's how you represent that memory write, correct? A. Yes.

Similarly, each of the Firewalls in combination with FMC infringes the '806 Patent. Tr. at 571:17-572:3. The FMC includes the TID that will receive threat intelligence feeds and operationalize this threat intelligence into rules for the Firewalls. Tr. at 673:21-675:25. The Firewalls implement the rule changes using Transaction Commit Model, which does not drop packets as the rules are switched. PTX-1196 at 1, 7; Tr. at 694:22-696:12, 698:8-22, 705:15-707:1.

As demonstrated by the trial record and outlined in Centripetal's Renewed Findings of Fact and Conclusions of Law, Cisco could not contest infringement of the '806 Patent given its admissions and technical documents.

C. Cisco Infringes Claims 11 and 21 of the '176 Patent

The '176 Patent, referred to as the "Correlation Patent" at trial, came from Centripetal's recognition that it could identify malware-infected computers on a network through "correlation" techniques. Tr. at 341:3-15. Centripetal's technology correlates logs corresponding to network traffic to identify and remediate unusual activity using network security rules. Tr. at 973:16-975:16. The '176 Patent increases the utility of otherwise commodity hardware of traditional switches and routers by transforming them into systems that can play a vital role in network security by sensing and reacting to network threats. Tr. at 341:21-342:10; Tr. at 973:19-974:22.

Centripetal's expert, Dr. Cole, relied on fifteen (15) Cisco technical documents to demonstrate that the Catalyst 9000 Switch or ISR/ASR Router with Stealthwatch infringes the '176 Patent. Tr. at 975:19-21. It is undisputed that Cisco's Catalyst 9000 Switch and ISR/ASR Router generate data about individual packets referred to as NetFlow and Syslogs with information from the transmitted packets, at the ingress and egress of the device. Tr. at 977:18-25, 984:5-13, 986:12-987:1, 988:12-22; PTX-1060 at 8, 23; PTX-572 at 762. It was not until April 2018, however, when CTA was updated, that it had the ability to use NetFlow and Syslog

logs to correlate the network traffic. PTX-1009 at 9; Tr. at 998:3-17. CTA enabled Stealthwatch to analyze and correlate the ingress and egress records of NetFlow and/or Syslog information sent by the Catalyst 9000 Switch and ISR/ASR Router to provide a detailed overview of all traffic occurring on the network. PTX-1065 at 005. CTA can use the correlated data to detect malicious threats to the network's security. PTX-1009 at 9; PTX-591 at 522; *see also* Tr. at 997:7-12 (identifying that NetFlow telemetry is another way of saying NetFlow log).

Cisco disputes that Stealthwatch correlates packets using NetFlow or Syslog records. The evidence at trial, however, confirms that Stealthwatch does exactly that:

Stealthwatch integrates with Cognitive Analytics ("CA" – aka Cognitive Threat Analytics). This involves the addition of a new information panel on the SMC's WebUI, and enhances Stealthwatch further by leveraging CA's cloud based analytics engine, that correlates threat behaviors seen in the enterprise with those seen globally. It uses machine learning and statistical modeling to learn from what it sees and adapt to changing network behavior over time.

Stealthwatch will then correlate the received syslog and relates it to the flows collected from network devices before and after the proxy, providing deeper visibility into customers web traffic.

PTX-1065 at 5; *see also* Tr. at 1108:6-1109:19, 1116:6-1117:1 (testifying that "correlation can be performed just of the NetFlow data," including "the ingress and egress data"); Tr. at 2149:13-18 (Cisco's engineer, Daniel Llewallyn, confirmed that Stealthwatch collects and correlates NetFlow records from multiple Catalyst 9000 Switches or ISR/ASR Routers within a network).

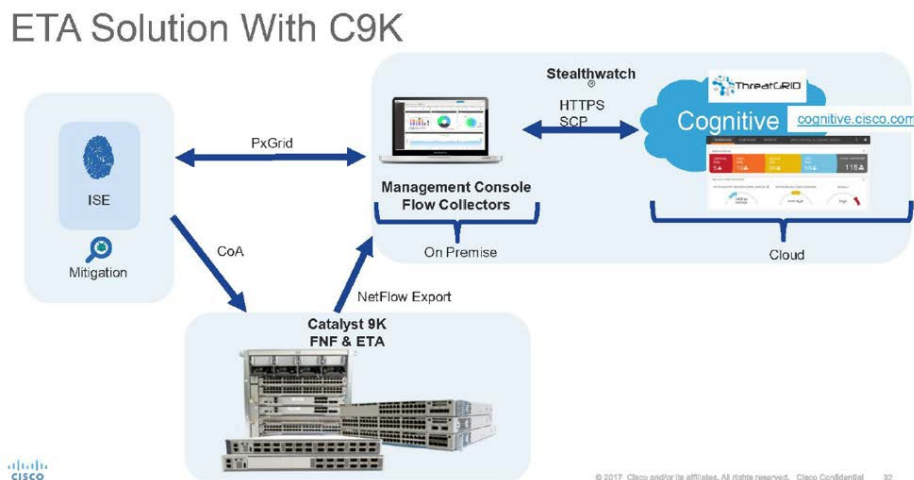
As demonstrated by the trial record and outlined in Centripetal's Renewed Findings of Fact and Conclusions of Law, Cisco could not contest infringement of the '176 Patent given the explicit admissions by its witnesses and in its technical documents.

D. Cisco Infringes Claims 24 and 25 of the '856 Patent

The '856 Patent, referred to as the "Encrypted Traffic Patent" at trial, addresses a fundamental issue related to the increased use of encryption, namely, that encryption provides privacy, but also allows cybercriminals to hide dangerous malware. '856 Patent at 1:17-20; Tr. at

310:20-23, 884:22-25, 889:6-12. In the '856 Patent, Centripetal invented a technology that allowed it to detect and block these threats in encrypted network traffic, without using the traditional slow and computationally expensive process of decrypting, inspecting, and re-encrypting packets. Tr. at 347:6-9, 347:13-348:16, 887:4-17.

Dr. Cole relied on twenty-seven (27) technical documents and Cisco's engineers' testimony to demonstrate that Cisco's Catalyst 9000 Switch and ISR/ASR Router with Stealthwatch and ISE infringe the '856 Patent starting in 2017 when Cisco launched its ETA technology. Tr. at 887:23-890:22; PTX-561 at 630. ETA allows network packets to be analyzed and blocked (if malicious) without decryption. Cisco's own technical documents outline the flow:



PTX-989 at 33.

Cisco's Catalyst 9000 Switch or ISR/ASR Router determines whether the traffic is encrypted or unencrypted. Tr. at 910:5-17, 944:16-945:1, 1064:8-14; PTX-989 at 4, 33 (Cisco "enhanced the network as a sensor to detect malicious patterns in not only non-encrypted traffic but also in encrypted traffic"); PTX-1849 at 244 (source code confirming that there is a determination made whether the packet flow is encrypted or unencrypted). After this, the

unencrypted portions related to encrypted packets are sent via NetFlow logs to Stealthwatch for analytics. Tr. at 910:5-911:9, 1078:7-18, 1082:16-24, PTX-989 at 33; PTX-578 at 61 (noting that ETA “[m]ake[s] the most of the unencrypted fields” in the encrypted packet).

Stealthwatch analyzes the NetFlow records from the packets and identifies malware threats in encrypted traffic without running any form of standard decryption. Tr. at 910:5-911:9, 936:4-20, 940:17-941:8; PTX-989 at 33; PTX-1010 at 1 (stating Stealthwatch “can detect malware in encrypted traffic without any decryption using Encryption Traffic Analytics.”); PTX-1009 at 12 (stating that ETA “[e]nhances existing Stealthwatch / CTA integration with malware detection capability for encrypted traffic without decryption.”). Stealthwatch receives real-time threat intelligence from third parties, as well as from Cisco’s Talos. Tr. at 912:14-22, 921:11-20, 926:21-927:10; PTX-20 at 1; PTX-1081 at 13; PTX-1926. Stealthwatch filters the NetFlow records to determine if any of the encrypted traffic in the network matches any known malicious signatures based on the NetFlow records, such as Initial Data Packet (IDP), Server Name Indicator (SNI), or Transport Layer Security (TLS). Tr. at 920:22-921:10, 956:3-958:8, 1054:15-20; PTX-1009 at 12; PTX-996 at 5. Stealthwatch sends the results of its analysis to ISE. Tr. at 910:5-911:9; PTX-989 at 33. ISE will provision rules for a change of authorization to the Catalyst 9000 Switch or ISR/ASR Router. Tr. at 1963:1-1964:25. If encrypted traffic is found malicious, the change in authorization by the ISE causes the packets to be routed to the null interface, a proxy system that drops the packets. Tr. at 963:25-966:19, PTX-256 at 082, 083; *see also* Tr. at 2199:21-2203:25.

Cisco’s defenses are divorced from the claims and the record. Cisco tries to dispute that the Catalyst 9000 Switch and ISR/ASR Router make their determinations with ETA “based on a portion of the unencrypted data” of the packets identified as encrypted (’856 Patent at 29:3-7).

This does not hold up, as Stealthwatch analyzes several categories of unencrypted data from the packets, including an initial data packet and the encryption “handshake.” PTX-561 at 630.

Contrary to Cisco’s contention that Stealthwatch cannot filter packets, Centripetal’s expert showed how “the entirety of this system, the routers and switches, the Stealthwatch and the Identity Service Engine” filter packets by blocking a flow. Tr. at 1119:2-9. He explained that once Stealthwatch identified a threat, “it would communicate with [ISE], it would then have the [Catalyst 9000 Switch or ISR/ASR Router] send the additional packets as part of that session to that proxy, the null interface, and then that would contain or control the damage that was being caused by that session.” Tr. at 1119:10-23, 910:5-912:12, PTX-989 at 1, 4, 24, 33. As Cisco’s expert confirmed, malware threats in encrypted network traffic require an *entire* packet flow (*i.e.*, thousands or even millions of packets) to reach its destination for reassembly. Tr. at 103:9-104:15. ETA in Stealthwatch analyzes unencrypted information to identify the entire packet flow, and—according to a Cisco document—“[u]pon discovery, *a malicious encrypted flow can be blocked or quarantined* by Stealthwatch.” PTX-584 at 398, 402, 403 (emphasis added); *see also* PTX-482 at 664-665 (Stealthwatch data sheet stating “[c]atch them in the act” and “detect and respond to threats in real time”). Therefore, it is undisputed that this process filters packets.

As demonstrated by the trial record and outlined in Centripetal’s Renewed Findings of Fact and Conclusions of Law, Cisco could not contest infringement of the ’856 Patent given its admissions and technical documents.

IV. CENTRIPETAL’S ASSERTED PATENTS ARE VALID AND ENFORCEABLE

Centripetal’s patents are presumed valid, and Cisco has the burden of proving invalidity by clear and convincing evidence. 35 U.S.C. § 282; *Microsoft Corp. v. i4i Ltd. P’ship*, 564 U.S. 91, 95 (2011). Cisco has not come close to meeting its burden.

A. Cisco Took the Position at Trial that All of the Accused Products Used Old Technology

Cisco's experts argued at trial that the products accused of infringing Centripetal's patents had the same technology as the earlier versions of Cisco's products. To advance this position, Cisco ignored its own documents demonstrating that this technology was new and implemented after meeting with Centripetal and after the priority date of all the patents, such that the older products could not contain the infringing technology.

For the '193 Patent, Cisco's expert, Dr. Crovella, relied on what it calls Cisco's Cyber Threat Defense System ("CTDS"), which consists of (1) a prior art Cisco router, Catalyst switch, or ASA firewall, (2) Lancope Stealthwatch Enterprise⁴ (running software version 6.2 or 6.3), and (3) Identity Services Engine (ISE) (running software version 1.1). However, Cisco failed to show that the same enhanced Quarantine functionality accused of infringing existed in CTDS. Tr. at 3008:17-3012:2 (Centripetal's expert, Dr. Orso, explaining that "quarantining functionality" relied upon by Dr. Crovella relates to shutting down an endpoint, not to the later added functionality of allowing certain types of data transfers while preventing others); DTX-711 at 2 (stating the "Shutdown port of the endpoint," which shows that quarantining involves shutting down the endpoint in CTDS); *see also* Tr. at 2437:15-17 (Dr. Crovella stating that the prior art also involved a human operator).

For the '806 Patent, Cisco's expert, Dr. Reddy, relied on Catalyst 6500 series Supervisor Engine 2T (e.g., Sup 2T models VS-S2T-10G and VS-S2T-10G-XL) running IOS Release 12.2(50)SY and Cisco Prime ("Catalyst 6500"). However, the accused functionality for accused Catalyst 9000 Switch and ISR/ASR Router involves FED 2.0 Hitless ACL, which was not

⁴ As noted at trial, Stealthwatch was a third-party product made by Lancope until Cisco acquired Lancope in 2015. Tr. at 1701:14-21.

developed by Cisco until 2017 according to their own documents. PTX-1195 at 1 (showing initial date of July 2017).

For the '176 Patent, Cisco's expert, Dr. Almeroth, relied on (1) a prior art Cisco router, Catalyst switch and (2) Lancope Stealthwatch Enterprise version 6.5.4. Tr. at 2308:11-23 (Dr. Almeroth testifying that he relies on Stealthwatch 6.5.4 released in 2014). At trial, Cisco's engineer, Mr. Llewallyn, testified that the accused CTA functionality was not added to Stealthwatch until version 6.10.3 in 2017. Tr. at 2148:8-11.

For the '856 Patent, Cisco's expert, Dr. Schmidt, relied on (1) Lancope Stealthwatch Enterprise versions 6.3, 6.5.4, and 6.5.5 and (2) ISE version 1.3. However, none of the documents he relied upon includes the word encryption. *See e.g.*, DTX-311, DTX-343, DTX-364, DTX-380, DTX-993. Indeed, the accused functionalities of ETA and CTA were not introduced until 2017. *See, e.g.*, Tr. at 2148:8-11 (Mr. Llewallyn testifying that CTA was not introduced until 2017). Accordingly, Cisco's argument that if they are found to infringe, the patents would be invalid is baseless because the alleged prior art systems did not have the accused functionality.

B. The Asserted Claims Are Valid Because Cisco Failed to Address Claim Elements

Cisco does not have any clear and convincing evidence that the asserted claims of Centripetal's Patents are invalid. As discussed above, Cisco's experts rely on prior versions of Cisco's products alone or in combination with third-party products as prior art. As noted at trial, the accused infringing functionality was not introduced until after Cisco met with Centripetal and after the priority dates of the asserted patents. As a result of Cisco's reliance on prior art products that do not have the infringing functionality, Cisco's experts had to ignore certain claim elements. For each of the asserted claims, Cisco's experts did not address claim elements or map

them to the prior art product and this deficiency is fatal to its invalidity theories.

1. The '193 Patent is Valid

For the '193 Patent, Dr. Crovella did not identify the claimed “operator” in the alleged prior art system, CTDS. *See* Tr. at 2427:14-2494:19; Tr. at 3012:3-3015:3 (Dr. Orso explaining that Dr. Crovella failed to identify an operator and noting that Cisco failed to identify an operator in its IPR petition for the '193 Patent). His conclusory testimony regarding the second “responsive to ...” element, including the “applying ... a second operator ...” and the “forwarding ...” elements is a far cry from proving that these elements with clear and convincing evidence. Tr. at 2464:22-2465:6; Tr. at 3015:8-18 (Dr. Orso identifying that Dr. Crovella failed to address “responsive to”), 3016:7-1317:10. Dr. Crovella did not explain how these elements are purportedly met, and his opinion cannot support a finding of anticipation or obviousness.

2. The '806 Patent is Valid

Cisco did not prove that the alleged prior art system of the Catalyst 6500 receives multiple rule sets and preprocesses those rule sets to optimize their performance to process packets as in the '806 Patent. Dr. Reddy, did not discuss the “receiving” and “preprocessing” claim elements, nor did he identify any corresponding functionality in the prior art system. Tr. at 3041:19-3043:24. As discussed above, Hitless ACL for FED 2.0 was the accused functionality added to the accused switches and routers which prevented packet loss. In contrast, the earlier version of Hitless ACL would drop packets because it would swap rules during packet processing. Tr. at 3034:23-3035:15, 3040:2-12; PTX-1195 at 3 (“Currently whenever there is a change to the ACE in an ACL, the data will drop packets during the change to hardware programming.”). Dr. Reddy also agreed that the accused functionality related to Hitless ACL was not released until 2017, after the priority date of the '806 Patent. Tr. at 2679:9-15.

3. The '176 Patent is Valid

For the '176 Patent, Cisco failed to show the Lancop Stealthwatch Enterprise version 6.5.4 met the “correlate, based on the plurality of log entries... received by the network device” element. Dr. Almeroth ignored the claim language, which requires correlating a plurality of log entries, and, instead, testified that the Netflow record was correlated with identity information from ISE, which is not a log entry. Tr. at 2320:15-2321:6. The prior versions of Stealthwatch had no correlation functionality until CTA was added beginning in late 2017. PTX-1893 at 11 (explaining new correlation feature in Stealthwatch 7.0); PTX-1065 at 5; PTX-569 at 272; PTX-595 at 179. Centripetal’s expert, Dr. Jaeger, explained that the earlier version of Stealthwatch focused on visibility and alarms, not correlation. *See, e.g.*, Tr. at 3152:13-22, 3154:6-25; DTX-343 at 1; DTX-463 at 14. While Dr. Almeroth argued that this earlier version of Stealthwatch would correlate something called “SLIC Feeds” with a Netflow record, he did not offer any evidence that the SLIC Feeds have a relationship with Netflow records. Tr. at 2323:7-2324:1. In fact, Cisco’s engineer testified that the SLIC Feeds do not correspond to packets received or transmitted by network devices. Tr. at 2167:15-21.

4. The '856 Patent is Valid

For the '856 Patent, there was no evidence that the prior versions of Stealthwatch could identify packets comprising encrypted or unencrypted data. Further, Cisco failed to prove that the prior versions of Stealthwatch met the “determine...one or more network-threat indicators” element based on unencrypted data from an encrypted flow. Dr. Schmidt glossed over this element, incorrectly claiming this was already shown. Tr. at 2033:20-2034:14. In other words, he failed to show that prior versions of Stealthwatch identified threats in encrypted traffic *without* decryption. While he argued that prior versions of Stealthwatch had the ability to identify threats without decryption, Cisco’s own documents contradicted him. Tr. at 2110:17-2111:7; PTX-383

at 355 (ETA with Stealthwatch provided the “first and only solution in the industry that can detect malware in encrypted traffic without any decryption using Encrypted Traffic Analytics.”); *see also* PTX-452 at 648; PTX-1135 at 946-947. The only purported evidence Dr. Schmidt pointed to was three pages of a single document regarding CTDS, and none of those pages include the words “packet,” “unencrypted,” or “encrypted.” DTX-364 at 1, 2, 14.

C. Cisco’s Experts Are Not Credible Because They Applied Differing Claim Constructions

Cisco’s multiple technical experts presented conflicting opinions at trial, testifying that the scope of each patent was different between infringement (the alleged “Non-Infringement Opinions”) and invalidity (the alleged “Invalidity Opinions”). These mutually exclusive interpretations are improper as a matter of law because claims “must be construed in the identical way for both infringement and validity.” *Kimberly-Clark Corp. v. Johnson & Johnson*, 745 F.2d 1437, 1449 (Fed. Cir. 1984); *W.L. Gore & Assocs., Inc. v. Garlock, Inc.*, 842 F.2d 1275, 1279 (Fed. Cir. 1988) (“Having construed the claims one way for determining their validity, it is axiomatic that the claims must be construed in the same way for infringement.”).

Cisco’s technical experts repeatedly emphasized that their Invalidity Opinions differed from their Non-Infringement Opinions. For example, Dr. Almeroth admitted he used a different understanding of the asserted claims of the ’176 Patent for his Invalidity Opinion than for his Non-Infringement Opinion. Tr. at 2340:18-2341:3. He also testified that while the claims *would be valid* if he applied the same interpretation used for infringement for validity, he was “not offering opinions [for validity] under what [he] believe[s] is the proper claim scope.” Tr. at 2341:16-23. In other words, Dr. Almeroth, along with all of Cisco’s other technical experts, construed patents one way for infringement and a different way for validity. Dr. Schmidt also confirmed that his Invalidity Opinion for the ’856 Patent only existed in a “hypothetical world”

driven by the Court's legal conclusions about infringement. *See, e.g.*, Tr. at 1982:22-1984:3, 2030:10-20, 2042:12-20, 2049:12-20. Dr. Reddy testified that he applied different interpretations for his invalidity versus non-infringement opinions for the '806 Patent. Tr. at 2675:14-2676:15.

It is legally improper for Cisco to pursue a broad construction for invalidity (even under the guise that it is "hypothetical"), while simultaneously using a narrow construction for non-infringement, which it did with the same expert. Such a tactic casts a cloud over the credibility and reliability of Cisco's expert opinions, which reflect litigation-driven alternative legal arguments, not scientific analysis. Cisco is not entitled to "adopt a 'heads I win, tails you lose' approach" to the core issues of the case, which another court observed "mak[es] it impossible for the [finder of fact] to ever reliably determine the results of the coin flip in the first place." *Miller v. Genie Indus., Inc.*, No. 3:10-cv-00063-MPM-SAA, 2012 WL 161408, at *3-4 (N.D. Miss. Jan. 19, 2012). Cisco's approach in this case is no different and certainly no more reliable.

D. Cisco Defense of Written Description Fails

1. Written Description Defense Requires a POSITA

Cisco's written description defense is baseless because Cisco did not address the requisite evidence of who a POSITA was to determine whether such an individual would have understood the patent at the relevant time. *Alcon Rsch. Ltd. v. Barr Labs., Inc.*, 745 F.3d 1180, 1191-92 (Fed. Cir. 2014) (reversing finding of lack of written description because defendant offered no evidence of whether a skilled artisan would have understood the patent at the relevant time); *Serby v. First Alert, Inc.*, 134 F. Supp. 3d 668, 680 (E.D.N.Y. 2015) (denying written description defense after bench trial "[b]ecause Defendants provide no evidence that the written description is insufficient to be understandable by a person of ordinary skill in the art"), *vacated on other grounds*, 664 F. App'x 105 (2d Cir. 2016), *as amended* (Dec. 22, 2016).

Because Cisco never addressed who a POSITA was, Cisco could not address whether

Centripetal’s Patent specifications permit *one of ordinary skill in the art* to determine that “the inventor had possession of the claimed subject matter as of the filing date,” a burden that Cisco has to address with clear and convincing evidence. *Streck, Inc. v. Rsch. & Diagnostic Sys., Inc.*, 665 F.3d 1269, 1285 (Fed. Cir. 2012) (affirming summary judgment order finding patents satisfied written description requirement as a matter of law) (citation omitted); *Biogen Int’l GmbH v. Mylan Pharms. Inc.*, 18 F.4th 1333, 1341 (Fed. Cir. 2021) (invalidity by written description requires clear and convincing evidence). Cisco offered no evidence “to establish ‘what an ordinarily skilled artisan would have known at the time the patent was filed’” and never “established whether or not one skilled in the art could ‘conclude that the inventor invented the claimed invention as of the filing date sought,’” which is a failure of proof. *See, e.g., Serby*, 134 F. Supp. 3d at 679-80 (ruling against written description defense after bench trial “[b]ecause Defendants provide no evidence that the written description is insufficient to be understandable by a person of ordinary skill in the art”) (citations omitted). Thus, Cisco’s opinion on lack of written description fails.

2. The ’856 and ’176 Patents Convey with “Reasonable Certainty” All Claims Elements

The challenged terms are valid because the specifications “‘convey with reasonable clarity to those skilled in the art that, as of the filing date sought, [Centripetal] was in possession of the invention,’ and demonstrate that by disclosure in the specification of the patent.” *Idenix Pharms. LLC v. Gilead Scis. Inc.*, 941 F.3d 1149, 1163 (Fed. Cir. 2019) (citations omitted).

For the ’176 Patent, Cisco disputes written descriptions of the “correlate ...” and the “responsive to ...” elements. Dr. Almeroth’s only argument is that the specification does not mention specific technologies used in the infringing products, such as CTA, machine learning, artificial intelligence, integrating threat feeds, or Netflow for the “correlate” and “responsive to”

elements. Tr. at 2333:22-2334:12. Cisco is therefore making the nonsensical argument that the exact infringing products needed to be disclosed when they did not exist yet. Here, the '176 Patent specification supports these terms as it specifically discloses using logs to correlate packets and, in response to the correlating, identifying hosts associated with malicious entities and communicating messages identifying that host. '176 Patent at 8:46-63, 12:55-13:13; Tr. at 3155:11-18, 3156:9-3157:14 (Dr. Jaeger identifying support for written description).

For the '856 Patent, Dr. Schmidt argues that the specification does not mention "NetFlow," thus fails for lack of written description. The '856 Patent's specification describes what is covered, which would include NetFlow, as it states that the "Packet-filtering system may be configured to correlate packets identified by the packet-filtering system with packets previously identified by packet-filtering system based on data stored in logs" '856 Patent at 5:20-30; *see also id.* at 5:31-56; Tr. at 3143:20-3144:21 (Dr. Jaeger discussing written description). In other words, the specification discloses the use of logs and logging of certain information from packets, which is what a Netflow record is.

V. CENTRIPETAL IS ENTITLED TO RELIEF FOR CISCO'S WILLFUL INFRINGEMENT

A. Centripetal Demonstrated a Reasonable Royalty Apportioned to the Footprint of the Invention

Centripetal demonstrated it was entitled to a reasonable royalty of 8% to 10% of the apportioned revenues for the Accused Products, based on robust expert analysis of the evidence, and in light of the *Georgia-Pacific* factors and a comparable license. 35 U.S.C. § 284; Tr. at 1443:5-11 (total damages from June 2017 to December 2019 would range from \$444 million to \$555 million); Tr. at 1443:17-1525:25 (detailed *Georgia-Pacific* analysis); PTX-1933. Damages for the period from June 2017 to March 2023 would range from approximately [REDACTED] based on Cisco's worldwide revenues or [REDACTED] based on U.S. revenues. PTX-1958.

Royalty Base. Centripetal's royalty base is the apportioned revenues from Cisco's infringing sales of the Accused Products. Cisco offers for sale and sells the Accused Products as integrated systems that provide network security functionality "of critical importance" to Cisco and its customers. *See, e.g.*, Tr. at 1453:22-1454:24, 1461:20-1464:13, 1464:18-1466:17, 1472:17-25, 1499:18-1500:10, 1525:10-25. Cisco markets and sells its products as a "cybersecurity architecture" and "as one product" based on Cisco's SEC statements, presentations, and technical marketing materials. *Id.* (explaining evidence such as PTX-1248 at 265-266; PTX-1507 at 494-495; PTX-560 at 768, 771; PTX-31 at 6); *see also* Tr. at 908:11-911:9 (describing system architecture with PTX-989 at 33); Tr. 440-441:14 (citing PTX-1260 at 849); PTX-197 at 196, 207. Cisco's technical expert confirmed that customers need Cisco's "comprehensive technique" and "[c]omprehensive set of products." Tr. at 2130:7-20.

Notwithstanding all the evidence, Cisco claimed there was insufficient proof that its products were sold in the infringing combinations. However, it never identified any credible rebuttal evidence to suggest the royalty base included non-infringing sales. Cisco simply excluded from its proposed royalty base all revenues from Switches, Routers, and Firewalls. Tr. at 2937:5-25 (Cisco's damages expert Dr. Becker admitting he excluded Switch and Router revenue from damages for the '193 Patent, where the Switches and Routers are accused without other products); Tr. at 2938:1-15 (Dr. Becker admitting he did not include Switch, Router, or Firewall revenue for any patent). Noting the "tremendous" disparity between the parties' damages calculations and Centripetal's unrebutted evidence, the court gave Cisco another opportunity *after the close of all evidence* to provide rebuttal evidence that its products were not sold as integrated systems and demonstrating "what [Cisco] considered to be the relevant products." Tr. at 2970:23-2971:4, 2976:11-2977:17. It even invited Cisco to provide anything

“you think would be helpful” because “you’re not limited by what I ask for.” Tr. at 2976:11-2977:17. Despite this extraordinary request and having several weeks to comply, Cisco produced no supportive data. In addition to lacking factual support, it defies common sense that a company could “advertise[] and sell[] all the accused products as part of the [Cisco] system” and “frequently highlight[] compatibility between system elements,” but escape direct infringement by separately selling the system’s constituent parts. *See Immersion Corp. v. Sony Comput. Ent. Am., Inc.*, No. C 02-0710 CW, 2005 U.S. Dist. LEXIS 4777, at *16, *23-24 (N.D. Cal. Jan. 10, 2005) (affirming damages with royalty base of accused product sales).

Apportioned Base Revenues. Centripetal apportioned the revenues in its royalty base by separated infringing and non-infringing product functions. Centripetal’s expert, Dr. Striegel, performed a technical apportionment approved of in *Finjan, Inc. v. Blue Coat Sys., Inc.*, 879 F.3d 1299, 1313 (Fed. Cir. 2018). Under this methodology, Dr. Striegel, a computer scientist, evaluated infringing functions versus non-infringing functions to identify what percentage of each accused product infringed each Asserted Patent. Dr. Striegel reviewed Cisco’s technical documents, depositions, and source code, and discussed infringement with Centripetal’s other technical experts. Tr. at 1337:17-1338:15. Next, he identified “core” functions, *i.e.*, the essential components of each product as perceived by a network and security expert with an extensive engineering background, using Cisco’s documents to inform what Cisco conveys to customers as “the key benefits, . . . the features, what should you expect if you were to go out and purchase this product.” Tr. at 1338:16-1339:24, 1427:24-1429:2. He thus distilled Cisco’s complex technology into generally-named functions for ease of reference and categorized certain components as “commodity components.” Tr. at 1345:11-22, 1428:12-22. Like the technical expert in *Blue Coat*, Dr. Striegel separated infringing and non-infringing functions on a patent-

by-patent and product-by-product basis for apportionment. Tr. at 1375:20-1376:16, 1401:14-1402:11; PTX-1931. For example, he excluded non-infringing, commodity-type functions, such as life-cycle management, ports, power supplies, cables, maintenance and operating systems. Tr. at 1376:6-16, 1407:4-19, 1430:13-18. Since Dr. Striegel apportioned by patent and product, apportioned damages are identifiable by patent and product.

Apportioned Royalty Rate. Centripetal also offered an inherently-apportioned royalty rate through reliance on the technically and economically comparable license between Centripetal and Keysight. This license applies its specified royalty rates to unapportioned revenues of licensed products. PTX-1125 at 493-494; Tr. 1564:2-21. “[W]hen a sufficiently comparable license is used as the basis for determining the appropriate royalty, further apportionment may not necessarily be required,” because in such circumstances, apportionment is “built-in.” *Vectura Ltd. v. GlaxoSmithKline LLC*, 981 F.3d 1030, 1040 (Fed. Cir. 2020) (citations omitted). In *Vectura*, the Federal Circuit affirmed a reasonable royalty of 3% applied to total (unapportioned) infringing revenues, holding that apportionment was “built-in” through the use of a comparable license that likewise applied a royalty rate to an unapportioned revenue base. *Id.*; *Elbit Sys. Land & C4I Ltd. v. Hughes Network Sys., LLC*, 927 F.3d 1292, 1301 (Fed. Cir. 2019) (affirming damages award with built-in apportionment). Such is the case here, given the close comparability of the Keysight agreement, which applied the specified royalty rates to the entire revenue base.

Mr. Gunderson explained that his reasonable royalty analysis, when compared apples-to-apples with the Keysight license royalty, yields an effective royalty rate of 2.7% to 3.3% of Cisco’s unapportioned revenues. Tr. at 1564:2-1565:17. This rate is roughly a third of the 10% rate in the Keysight license. *Id.* If the base for the hypothetical license is kept the same as in the

Keysight license—*i.e.*, unapportioned—then the reduced 2.7% to 3.3% rate fully accounts for the differences between the agreement and the hypothetical negotiation. Thus, further apportionment—and specifically, apportionment of the revenue base—is not required.

B. Cisco’s Willful Infringement Warrants Additional Relief, including Enhanced Damages and a Permanent Injunction

Cisco does not deny that it had pre-suit knowledge of Centripetal’s Asserted Patents and even asked about Centripetal’s patents. *See supra* Section II(B)-(D) (Centripetal gave Cisco detailed presentations of the patents and their functionality, including numerous demonstrations of its marked RuleGATE product); PTX-102 at 1. After learning of Centripetal’s algorithms and internally stating it should undertake a “study [of Centripetal’s patent] claims,” Cisco released its infringing products. PTX-134 at 3; *see also Halo Elecs., Inc. v. Pulse Elecs., Inc.*, 579 U.S. 93, 100-03, 105-08 (2016); *WesternGeco L.L.C. v. ION Geophysical Corp.*, 837 F.3d 1358, 1363 (Fed. Cir. 2016). Thus, the evidence demonstrates that Cisco’s infringement was willful.

Centripetal seeks enhanced damages for Cisco’s willful and continuing infringement under 35 U.S.C. § 284. When considering an award of enhanced damages, courts use the “non-exclusive factors articulated in *Read Corp. v. Portec, Inc.*, 970 F.2d 816 (Fed. Cir. 1992).” *Georgetown Rail Equip. Co. v. Holland L.P.*, 867 F.3d 1229, 1244-45 (Fed. Cir. 2017) (affirming substantial evidence supported willfulness finding and there was no abuse of discretion in enhancing damages). Cisco never offered evidence that it investigated or formed a good-faith belief of invalidity or non-infringement. Rather, Cisco only sought information from Centripetal, pretending it would purchase the technology or partner with Centripetal. *Supra*, Section II(C). Cisco, the world’s largest networking company, successfully used Centripetal’s patented technology to avoid commoditization and introduce cutting-edge security into its products, and substantially increased its sales in doing so. Tr. at 1607:22-1608:18, 3435:4-3438:24 (revenues

generally increased after release of infringing technology). During the course of litigation, Cisco attempted to use its experts to rewrite its own documents and engineer testimony. *Supra*, Section II(D). It thus failed to present plausible non-infringement positions and still infringes today.

Centripetal seeks a permanent injunction enjoining Cisco from making, using, offering for sale, selling, and/or importing its infringing Firewalls.⁵ Centripetal's RuleGATE directly competes with Cisco's Firewalls, and Centripetal demonstrated at trial that it has suffered irreparable harm from Cisco's infringement. For example, Centripetal lost market share to Cisco and others in the market following Cisco's lead and suffered reputational harm because Cisco usurped Centripetal's position at the forefront of the market. *See, e.g.*, Tr. at 1209:12-1210:20, 1246:19-1247:19 (Jonathan Rogers' testimony); Tr. 1331:15-1332:2 (Centripetal's VP of Sales testifying about encountering Cisco in the marketplace); *see also* Tr. at 3464:8-14 (Cisco revenues increased after the release of infringing technology). Moreover, the public interest and the balance of hardships between the parties favor an injunction because such relief would significantly impact Centripetal's business, which is ready to meet public demand for its technology that is more capable than Cisco's Firewalls, and only minimally impact Cisco, which has expansive product offerings and is primarily focused on networking as opposed to security.

VI. CONCLUSION

Centripetal has proven that Cisco willfully infringes the Asserted Patents and should receive at least a reasonable royalty and other relief as the Court finds appropriate.

⁵ To the extent Cisco continues to use Centripetal's patented technology, Cisco should be required to pay an enhanced royalty for its continued use.

Dated: May 26, 2023

Respectfully submitted,

/s/ Stephen E. Noona

Stephen Edward Noona
Virginia State Bar No. 25367
KAUFMAN & CANOLES, P.C.
150 W Main St., Suite 2100
Norfolk, VA 23510
Telephone: (757) 624-3239
Facsimile: (888) 360-9092
senoona@kaufcan.com

Paul J. Andre
Lisa Kobialka
James Hannah
Hannah Lee
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
333 Twin Dolphin Drive, Suite 700
Redwood Shores, CA 94065
Telephone: (650) 752-1700
Facsimile: (650) 752-1800
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com
hlee@kramerlevin.com

Attorneys for Plaintiff
CENTRIPETAL NETWORKS, LLC

CERTIFICATE OF SERVICE

I hereby certify that on May 26, 2023, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will automatically send notification of electronic filing to all counsel of record.

/s/ Stephen E. Noona
Stephen E. Noona
Virginia State Bar No. 25367
KAUFMAN & CANOLES, P.C.
150 West Main Street, Suite 2100
Norfolk, VA 23510
Telephone: (757) 624-3239
Facsimile: (888) 360-9092
senoona@kaufcan.com